Attorney's. Docket No. 99-956

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D. C. 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of:

Inventors: Christopher Paul CARROLL

For: CRYPTOGRAPHIC TECHNIQUES FOR A
          COMMUNICATIONS NETWORK

Certification Under 37 CFR 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service on this date _____ in an envelope as "Express Mail Post Office to Addressee" mailing label EK673490845US addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Robert McHugh
_____
(typed or printed name of person mailing paper)
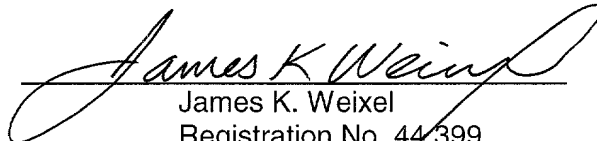
_____
(Signature of person mailing paper)

1

Attorney's Docket No.   99-956

Enclosed are:

[20]	pages of specification and cover sheet
[7]	pages of claims
[1]	page of abstract
[15]	sheets of formal drawings.
[2]	pages of declaration and power of attorney.
[2]	pages of assignment and assignment recordation form
[2]	pages of information disclosure statement
[1]	page of USPTO form 1449
[4]	references
[1]	return postcard

CLAIMS AS FILED				
	NUMBER FILED	NUMBER EXTRA	RATE	BASIC FEE $710.00
TOTAL CLAIMS	32 - 20	12x	$18	216.00
INDEPENDENT CLAIMS	5-3x	2x	$80	160.00
MULTIPLE DEPENDENT CLAIM(S)		0 x	$260.00	
		TOTAL FILING FEE		$1086.00

[x]   Please charge my Deposit Account No. 07-2339 in the amount of **$1086. This transmittal letter is submitted in duplicate.**

[x]   The Commissioner is hereby authorized to charge any additional fees under 37 CFR 1.16 and 1.17 which may be required by the papers submitted herewith or credit any overpayment to Account No. 07-2339.

James K. Weixel
Registration No. 44,399
Attorney for Applicant(s)

Verizon Services Group
600 Hidden Ridge, HQE03G13
Irving, TX 75038
Phone: (781) 466-2220
Fax: (781) 466-4021

UNITED STATES PATENT APPLICATION

OF

Christopher Paul CARROLL

FOR

CRYPTOGRAPHIC TECHNIQUES FOR A COMMUNICATIONS NETWORK

Related U.S. Applications

This application claims priority from U.S. Provisional
Patent Application Serial No. 60/165,539, entitled "THIRD
GENERATION WIRELESS COMMUNICATIONS AUTHENTICATION AND KEY
AGREEMENT MECHANISM OPTION", filed 11/15/99; and U.S.
Provisional Patent Application Serial No. 60/167,811,
entitled "THIRD GENERATION WIRELESS COMMUNICATIONS
AUTHENTICATION AND KEY AGREEMENT MECHANISM OPTION", filed
11/29/99. Both applications are incorporated by reference
herein in their entirety.

Background of the Invention

1.   Field of the Invention

The present invention relates generally to
cryptographic techniques for use in a communications
network such as a wireless communications network.

2.   Description of Related Art

First generation wireless communications networks were
based on analog technologies such as the Advanced Mobile
Phone Service (AMPS). Second generation wireless
communications networks introduced digital communications
technologies such as the Global System Mobile (GSM), IS-136
Time Division Multiple Access (TDMA), and IS-95 Code
Division Multiple Access (CDMA). Authentication and Key
Agreement (AKA) protocols were developed for first and
second generation networks to prevent theft of cellular

telephone service, to provide subscriber voice privacy, and provide other security features.

FIG. 1 illustrates a typical cellular telephone or Personal Communication Services (PCS) network. A

5   subscriber, using a Mobile Station (MS) 130 (e.g., a cellular phone), can roam outside of the area covered by their Home Environment (HE) 110 network and obtain wireless communications service from a Serving Network (SN) 120. The HE 110 and SN 120 networks typically include a switch,

10   base station, and other components (not shown), as is known in the art. As is known in the art, the HE 110, SN 120, and MS 130 are controlled by software, firmware, and/or hardware instructions.

The MS 130 often features a removable Universal

15   Subscriber Identity Module (USIM) that resides in the MS 130 to store subscriber information such as a subscriber's identity, secret key information, and so forth. To simplify descriptions herein, the USIM is considered part of MS 130. However, a subscriber can transfer their USIM

20   into other MS-s 130 to obtain service.

An AKA protocol for second generation wireless communication networks provides MS 130 to SN 120 authentication. In a typical GSM system, the HE 110 and MS 130 share a common 128-bit secret key K. To enable roaming

25   privacy and authentication, HE 110 passes an authentication vector including three pieces of cryptographic data to a SN 120. Each vector includes a random challenge, response, and privacy key.

When MS 130 requests service, SN 120 transmits the

30   random challenge over the air to the MS 130. MS 130 combines the random challenge with the secret key K using a cryptographic primitive (e.g., a hash function) to generate

the response. MS 130 transmits the response to SN 120
which compares the response value received from MS 130 with
the response value provided by HE 110. If the response
values are equal, SN 120 provides system access to MS 130.

5   MS 130 also uses the random challenge and K to create a
privacy key that is identical to the privacy key sent from
HE 110 to SN 120 as part of the cryptographic triplet.
With the same privacy key, SN 120 and MS 130 can securely
communicate. In this scheme, the SN 120 need not implement

10   a cryptographic primitive (e.g., a hash function).

A third generation AKA mechanism adopted by the Third
Generation Project Partners (3GPP) enhances the original
GSM AKA mechanism by enabling mutual authentication between
SN 120 and MS 130. The 3GPP AKA mechanism replaces the GSM

15   crypto-triplet vector with a crypto-quintet authentication
vector (AV) to facilitate MS/SN mutual authentication.

FIG. 2 illustrates formation of an AV by an HE 110.
As shown, the AV includes five components concatenated
together: (1) the random challenge (RAND), (2) an expected

20   response (XRES), (3) a cipher key (CK), (4) an integrity
key (IK), and (5) an authentication token (AUTN). AUTN
includes three components: (1) an exclusive-or of a
sequence number (SQN) and anonymity key (AK), (2) a MODE
value, and (3) a message authentication code (MAC). The

25   sequence number indicates the AVs position in a sequence of
AVs. Functions f1 through f5 are derived using a
cryptographic primitive shared between HE 110 and MS 130.
Different values of primitive constants or parameters
control which function, f1 through f5, the primitive

30   provides.

When roaming, a MS 130 may be authenticated each time
a MS 130 owner places a call. Thus, typically, an HE 110

sends multiple AVs to SN 120 to enable multiple
authentications between SN 120 and MS 130.

5

10

15

20

25

30

FIG. 3 illustrates SN 120 authentication in 3GPP AKA.
To authenticate SN 120, the MS 130 and HE 110 keep track of
counters SQN_{MS} and SQN_{HE}. When HE 110 generates an AV, SQN_{HE}
is incremented. MS 130 authentication of SN 120 is
performed by ensuring that SQN in each new AV is greater
than SQN in the previous AV. The MS 130 also verifies that
SQN_{HE} originated from the HE 110 by verifying the MAC in the
AUTN.

It is possible for the SQN counter in HE 110 and MS
120 to lose synchronization. For this reason, the 3GPP AKA
mechanism has SQN re-synchronization procedures. If K is
reset or replaced for a particular USIM, SQN can be reset
at the HE 110 and MS 130.

FIG. 4 illustrates the flow of a typical 3GPP AKA
mechanism. When MS 130 requests service from SN 120, SN
120 sends (step 202) an authentication request to HE 130.
Upon receiving the request associated with a particular MS
130, HE 110 generates (step 204) an array of AVs for that
particular MS 130. HE 110 sends (step 206) the AVs to SN
120 which, in turn, stores (step 208) the AVs in its
Visitor Location Register (VLR). SN 120 selects (step 210)
the first sequential AV(i) (e.g., i = 1) and sends (step
212) RAND(i) and AUTN(i) to MS 130. MS 130 verifies (step
214) AUTN(i) and computes RES(i). If SQN(i) is greater
than SQN_{MS}, MS 130 successfully authenticates SN 120. MS
130 sends (step 216) RES(i) to SN 120. SN 120 compares
(step 218) RES(i) with XRES(i). If RES and XRES are equal,
SN 120 has successfully authenticated MS 130. Finally, MS
130 computes (step 220) CK(i) and IK(i) while SN 120
selects CK(i) and IK(i).

FIG. 5 illustrates a cryptographic key hierarchy of the 3GPP AKA mechanism. A secret key K is the root secret shared only between the HE 110 and MS 130. Whenever mutual authentication is performed, a cipher key (CK) is generated

5 to facilitate voice and data privacy. Additionally, an integrity key (IK) is generated to facilitate message authentication.

The North American Telecommunications Industry Association (TIA) TR-45 standards group has based AKA on a

10 shared secret between HE 110, SN 120, and MS 130. In a TR-45 cellular/PCS network, HE 110 sends Shared Secret Data (SSD) to SN 120 to enable MS 130 to SN 120 authentication. SSD is derived from an Authentication key (A-key), shared between HE 110 and MS 130 only. The A-key is analogous to

15 the GSM secret key K. SSD consists of SSD-A, used for MS 130 challenge-response authentication, and SSD-B, used for SN/MS voice and data privacy. When MS 130 requests service from SN 120, HE 110 sends SSD to SN 120. With SSD, SN 120 can authenticate MS 130 until SSD is updated between HE 110

20 and MS 130.

Unlike a GSM network where SN 120 continuously requests new vectors of crypto-triplets to perform MS 130 authentication, SN 120 in a TR-45 network acquires unique SSD from HE 110 and uses SSD for the duration that MS 130

25 operates within the SN 120 area. Ideally, SSD update is performed between HE 110 and MS 130 after MS 130 leaves the SN 120 area to establish a new SSD, preventing SN 120 from knowing an SSD used by another service network. Unfortunately, many service providers do not update SSD

30 frequently, allowing many service providers to know SSD-A which is the authentication secret for TR-45 cellular telephones.

The TIA TR-45 is considering adoption of the 3GPP AKA for TR-45 networks to support global harmonization of wireless communication standards. To retain the advantages of using a shared secret like SSD, the TR-45 is considering

5   using the 3GPP IK key as SSD for third generation TR-45 wireless networks.

Additionally, the TR-45 is considering the adoption of the Long-term Enhanced Subscriber Authentication (LESA) AKA in which interlocking challenges provide mutual

10   authentication between SN 120 and MS 130. In the LESA AKA mechanism, SN 120 sends a random number R_N to MS 130. MS 130 generates a second random number R_M. MS 130 computes a response to SN 120 by combining R_N, R_M, and SSD in a cryptographic primitive. MS 130 sends the response and

15   random number R_M to SN 120. With R_M, SN 120 computes the same response, authenticating MS 130. Then SN 120 computes a second response for MS 130 by combining R_M and SSD in the cryptographic primitive. SN 120 sends the second response to MS 130. MS 130 verifies the second response,

20   authenticating SN 120.

Finally, 3GPP has considered an AKA mechanism similar to the LESA AKA, known as Authentication based on a Temporary Key (A-TK). The A-TK AKA mechanism uses a procedure of interlocking challenges between HE 110 and MS

25   130 to establish a temporary key (KT). Once KT is established, SN 120 uses traditional challenge-response to authenticate MS 130. MS 130 authentication of SN 120, however, is not performed explicitly, but is implicitly achieved by the establishment of CK and IK based on random

30   numbers provided by SN 120 and MS 130.

Summary of the Invention

Techniques are described for enabling authentication, key agreement, and/or encrypted communication between

5   communications network stations and service networks. The techniques described herein can include the negotiation and use of a cryptographic primitive shared between a service network and a home environment of a station. The techniques described also include use of a key usage

10   indicator, such as a sequence number, maintained by the service network and a station. Comparison of the key usage indicators can, for example, permit efficient authentication of the service network by the station without undue burden on a home environment network of the

15   station.

In general, in one aspect, the invention features a method for use in authenticating a service network to a station. The method includes storing a key at the service network and transmitting information to the station that

20   enables the station to compute the key stored at the service network. The method also includes receiving a request for service at the service network from the station, adjusting a value corresponding to key usage, and transmitting information corresponding to the value to the

25   station.

Embodiments may include one or more of the following features. The method may include receiving a vector of authentication information from the home environment network of the mobile station. The vector includes an

30   indication of the vector's position in a sequence of vectors. The information transmitted to the station that enables the station to compute the key stored at the

service network may include one or more portions of the
received vector of authentication information. The
received vector of authentication information can include
the key stored by the service network. The method may

5   further include computing, at the service network, the key
stored by the service network based on information included
in the received vector.

Adjusting a value indicating use of the key can
include incrementing a sequence number corresponding to a

10   number of times the key has been used. The method may
further include using the key to compute a cipher key for
encrypting communication between the service network and
the station. The method may also include negotiating use
of a cryptographic primitive between the service network

15   and the home environment network.

In general, in another aspect, the invention features
a method for use in authenticating a service network to a
station. The method includes computing a key, stored by
the service network, based on information received at the

20   station from the service network. The station maintains an
indicator of key usage. The method includes receiving at
the station an indicator of key usage maintained by the
service network and comparing the key usage indicator
maintained by the service network with the key usage

25   indicator maintained by the station.

Embodiments may include one or more of the following
features. The method may further include maintaining an
authentication vector sequence number at the station,
receiving at the station from the service network an

30   indication of an authentication vector sequence number
maintained by the home environment network, and comparing
the authentication vector sequence number maintained by the

8

home environment network with the received authentication
vector sequence number maintained by the station. The
method may include receiving from the service network
identification of a cryptographic primitive. The method

5   may include using the key to compute a cipher key for
encrypting communication between the service network and
the station.

In general, in another aspect, the invention features
a method for use in authentication in a communications

10   network including a home environment network, a service
network, and a station. The method includes determining at
the home environment network a cryptographic primitive
offered by the service network and transmitting to the
service network at least one vector of authentication

15   information corresponding to a particular station.

Embodiments may include one or more of the following
features. Determining may include receiving identification
of the cryptographic primitive from the service network,
for example, as a value of a MODE field. The vector of

20   authentication information may include an indication of an
authentication vector sequence number maintained by the
home environment network.

In general, in another aspect, the invention features
a method for use by a mobile station that can communicate

25   with different service networks. The method includes
storing different sets of cryptographic information for the
different respective service networks, selecting a set of
cryptographic information for one of the service networks,
and using the selected set of cryptographic information to

30   communicate with the service network.

Embodiments may include one or more of the following.
The sets of cryptographic information may include a key

shared by the station and the service network. The method

may include computing the key shared by the station and the

service network based on information received from the

service network. The sets of cryptographic information may

5   include an indicator of usage of the key. Using the

selected set of cryptographic information may include using

the selected set of cryptographic information in encrypting

communication between the station and the service network.

In general, in another aspect, the invention features

10   a method of handling authentication and key agreement in a

system including a home environment network, a service

network, and a mobile station in which the home environment

network and the mobile station share a secret key K. The

method includes determining whether the home environment

15   and the service network share a cryptographic primitive.

If it is determined that the home environment and the

service network do not share a cryptographic primitive, the

method handles authentication and key agreement between the

mobile station and the service network using 3GPP (Third

20   Generation Project Partners) AKA (authentication and key

agreement). If it is determined that the home environment

and the service network share a cryptographic primitive,

handling authentication and key agreement by computing a

shared secret key (SSK), transmitting information from the

25   service network to the station that enables the station to

compute the SSK, and

replacing the use of K in the 3GPP AKA with SSK.

Advantages will become apparent in view of the

following description, including the figures and the

30   claims.

Brief Description of the Drawings

FIG. 1 is a block diagram of a communications network according to the prior art;

FIG. 2 illustrates generation of an authentication vector according to the prior art;

FIG. 3 illustrates authentication of a service network according to the prior art;

FIG. 4 is a flow-chart of an authentication and key agreement process according to the prior art;

FIG. 5 illustrates a cryptographic key hierarchy according to the prior art;

FIG. 6 is a flowchart of an initial authentication and key agreement process used to generate a shared secret K;

FIG. 7 is a flowchart of a mutual authentication mechanism using a shared secret K;

FIG. 8 illustrates generation of an authentication token;

FIG. 9 illustrates authentication of a service network using a temporary sequence number;

FIG. 10 illustrates generation of a shared secret;

FIG. 11 illustrates a cryptographic key hierarchy;

FIG. 12 illustrates generation of a shared secret authentication vector by a home environment;

FIG. 13 illustrates a cryptographic key hierarchy;

FIG. 14 illustrates a mobile station straddling bordering cells of different service networks; and

FIG. 15 is a flowchart of a mobile station process for handling communication with a service network.

Detailed Description of the Preferred Embodiments

Described herein are techniques that can securely, efficiently, and robustly handle authentication and key

11

agreement in a communications network such as a wireless
communications network. In particular, the techniques
described herein can enhance traditional 3GPP AKA by giving
service providers the option to use traditional 3GPP AKA or

5   an optional AKA mechanism. The present invention is not
limited to wireless applications, and can also be used in
other networks such as electronic toll systems, internet
access terminals, cable TV and data networks, and other
networks in which a service provider allows subscribers to

10   use another service provider's network. For purposes of
the following description, the techniques are described
with respect to a wireless communications network.
However, the description should be understood as applying
to other networks or devices, such as the ones discussed

15   above.

         In one aspect, the invention features an optional 3GPP
AKA mechanism that can be used in conjunction with the
traditional 3GPP AKA. In the optional 3GPP AKA, a HE 110
and SN 120 share at least one common cryptographic

20   primitive. For example, HE 110 and SN 120 may both use
SHA-1 or MD-5 as a cryptographic hash function.

         The optional 3GPP AKA can include procedures that
allow for primitive negotiation, for example, between the
HE 110 and SN 120. For example, a one byte MODE field can

25   store data identifying the AKA cryptographic primitive or
set of AKA cryptographic primitives offered by an HE 110,
SN 120, or MS 120. For example, a MODE field value of "S"
can represent a request for communication using a shared
SHA-1 primitive. The SN 120 authentication data requests

30   can also include a primitive version identifier.

         As will be appreciated by those of skill in the art, a
field other than the MODE field may be used to facilitate

AKA primitive negotiation between elements of the
communication network. Additionally, as those of skill in
the art will appreciate, a wide variety of alternate
information exchanges can be used to negotiate a shared

5   primitive. For example, either the HE 110 or SN 120 may
initiate negotiation. Similarly, either the HE 110 or SN
120 may initially identify the cryptographic primitive(s)
it offers.

       If HE 110 and SN 120 do not share a common AKA

10   primitive (e.g., if HE 110 determines that it does not
provide the primitive identified in an SN 120 request for
AVs), standard 3GPP AKA is performed instead of the
optional 3GPP AKA mechanism described below. If HE 110 and
SN 120 share a common AKA primitive, the optional 3GPP AKA

15   mechanism, may be used to increase the efficiency of mutual
authentication between the MS 130 and SN 120.

       FIG. 6 illustrates the flow of an optional AKA
mechanism that can reduce the amount of Authentication
Vector (AV) traffic by establishing a Shared Secret K (SSK)

20   between the MS 130 and SN 120 using one AV. As shown, when
MS 130 requests service from SN 120, SN 120 sends (step
602) an authentication request to HE 130 indicating that a
common primitive is available. Upon receiving the request
associated with a particular MS 130 and noting the

25   indication of a shared primitive (e.g., HE 110 offers the
same primitive as indicated by the MODE field), HE 110
generates (step 604) at least one AV associated with that
particular MS 130. After generating (step 604) the AV, the
HE 110 sends (step 606) the AV to SN 120. SN 120 stores

30   the AV in its Visitor Location Register (VLR) and generates
(step 608) SSK(i). After initial communication,

communication between the SN 120 and MS 130 will depend on both computing the same SSK(i).

After selecting (step 610) an AV(i), SN 120 sends (step 612) RAND(i) and AUTN(i) of AV(i) to MS 130. MS 130

5   verifies AUTN(i) and computes (step 614) RES(i) (see FIG. 3). If SQN(i) is greater than SQN_{MS}, MS 130 successfully authenticates SN 120. MS 130 sends (step 616) RES(i) to SN 120. SN 120 then compares (step 618) RES(i) with XRES(i). If RES and XRES are equal, SN 120 has successfully

10   authenticated MS 130. Finally, MS 130 computes CK(i) and IK(i) while SN 120 selects (step 620) CK(i) and IK(i).

After establishing SSK and performing the initial AKA, the standard AKA protocol between SN 120 and MS/USIM 130 is modified by replacing K_i with SSK_i for AKA calculations

15   between the SN 120 and MS 130 for the duration of MS roaming. The protocol is further modified by using a Temporary SQN (TSQN) established between the SN 120 and MS/USIM 130 for the duration of MS 130 roaming in the SN 120 network area.

20   FIG. 7 illustrates how subsequent authentications are performed between SN 120 and MS 130, for example, in response to a MS 130 request for service from SN 120. SN 120 generates (step 702) RAND(i) and generates TAUTN(i) using SSK(i) (see FIG. 8). SN 120 sends (step 704) RAND(i)

25   and TAUTN(i) to MS 130, for example, with MODE = SHA-1. MS 130 verifies (step 706) TAUTN(i) and computes RES(i) (see FIG. 9). If $TSQN_{SN}(i)$ is greater than $TSQN_{MS/USIM}$, MS 130 successfully authenticates SN 120. MS 130 sends (step 708) RES(i) to SN 120. SN 120 compares (step 710) RES(i) with

30   XRES(i). If RES and XRES are equal, SN 120 has successfully authenticated MS 130. MS 130 computes (step

712) CK(i) and IK(i). SN 120 computes (step 714) CK(i) and
IK(i).

Just as SQN_i uniquely increments for a K_i, $TSQN_i$
uniquely increments for an SSK_i. Thus for a unique SSK, the
MS 130 maintains a uniquely incrementing TSQN to facilitate
mutual authentication between the MS 130 and SN 120. While
TSQN increments each time the same SSK is used for
communication between an SN and MS, TSQN increments for a
relatively short period of time compared with SQN,
lessening the chance mis-synchronization. Additionally,
TSQN need not impact the maintenance of SQN within the HE
110 and MS/USIM 130. TSQN can automatically reset when a
new SSK (associated with a particular SN 120 is formed.
This approach can eliminate the TR-45 problem of having to
update SSD.

As described above, TSQN is a sequence number.
However, other values indicating key usage may be featured.
For example, adjusting the value may feature decrementing
instead of incrementing a numeric value. Additionally, the
value need not be restricted to numbers but may instead
feature a character or boolean value.

A HE/SN pair, sharing a common primitive, can choose
to utilize this scheme if they desire. However, even if HE
110 and SN 120 share a common AKA primitive, the HE 110 can
utilize the standard 3GPP AKA mechanism and pass multiple
AVs to SN 120.

The HE 110 may pass one or more AVs to SN 120 with the
MODE value indicating standard 3GPP AKA. The SN 120,
however, after the initial standard AKA setup, can use a
common AKA primitive MODE value (e.g. SHA-1) to notify the
MS 130 to use SSK and TSQN when utilizing the modified 3GPP
AKA. Prior to initiating the optional AKA scheme, the SN

120 may determine if the MS 130 supports (e.g., includes instructions for) the optional scheme, for example, based on MS 130 identification information transmitted by the MS 120. Additionally, the MS 130 can transmit a message to

5 the SN 120 declining use of the optional scheme, for example, if the MS 130 does not provide the primitive identified by the SN 120 in the MODE field.

FIG. 10 illustrates an example of SSK generation. As shown, SSK can be generated using IK and RAND where f3 is

10 the generating function (e.g. SSK = $f3_{IK}(RAND)$). SSK may also be generated using a new function f6 derived from the shared cryptographic primitives(s) if desired.

FIG. 11 illustrates a cryptographic key hierarchy for the optional 3GPP AKA mechanism. A secret key K is the

15 root secret shared between the HE 110 and MS 130. When mutual authentication is first performed between SN 120 and MS 130, a CK is generated to facilitate voice and data privacy and an IK is generated to facilitate message authentication. SSK can be derived from IK using function

20 f3. For all subsequent SN 120 network accesses, CK and IK are derived from SSK.

FIG. 12 illustrates a different optional AKA mechanism. As shown, SSK may be generated using a new function f6 (e.g. SSK = $f6_K(RAND)$). When using the new

25 function, SSK can be generated by HE 110. HE 110 can include the generated SSK in the AV. With SSK included in the AV, the AV is defined as Shared Secret AV (SSAV). A SN 120 receiving SSAV can simply extract SSK instead of independently computing SSK. The MS 130, however, still

30 independently determines SSK from AV information transmitted by SN 120 to the MS 130.

After initial MS/SN mutual authentication and SSK
generation, the SN 120 and MS/USIM 130 use SSK and TSQN for
subsequent authentications as shown in Figure 7.
Resynchronization of TSQN is not necessary because SN 120

5   can query HE 110 for a new SSAV, perform standard 3GPP AKA
and establish a new SSK with a TSQN reset. The SN 130 may
request multiple AVs from the HE 110 initially to allow for
new SSK formation and TSQN reset.

FIG. 13 illustrates the cryptographic key hierarchy

10   when SSK is formed by HE 110 using RAND and K. Although
SSAV is larger than AV, HE 110 and SN 120 traffic is
reduced in comparison to the original 3GPP AKA mechanism
because only one SSAV is sent to SN 120 for roaming
authentication. By generating SSK from RAND and K, instead

15   of from RAND and IK, AKA mechanism security is improved.
Thus, SSK can be derived from IK for improved efficiency or
from K for improved security.

FIG. 14 illustrates another aspect of the invention
that provides support for border cell operations. As

20   shown, the MS 130 can store different cryptographic
elements (e.g., SSK/TSQN pairs) for different SNs 120. By
storing multiple SSK/TSQN pairs with each pair associated
with a different SN 120, the MS 130 can straddle the border
between multiple systems without requiring VLR-to-VLR AV

25   sharing, SSD sharing, or SSD update.

As shown in FIG. 14, MS 130 straddles between areas
served by two different serving networks. MS 130 uses
SSK_{SN-A} for service from serving network A (SN-A) and SSK_{SN-B}
for service from serving network B (SN-B). The MS 130 may

30   store identification of a SN and the respective SSK/TSQN
pair being used. Thereafter, the 130 may identify the SN
providing service to retrieve the appropriate pair.

SSK freshness depends on the SN 120 VLR and MS 130 rules. For example, the SN 120 may chose to store SSK for up to a week of inactivity. The MS 130 may store multiple SSK/TSQNs in a queue (five pairs or more) using first-in-

5   first-out (FIFO). This technique may be ideal for travelers moving between multiple systems and countries within a brief period of time. In the event the MS 130 deletes SSK_{SN-A} before SN-A deletes SSK_{SN-A}, the MS will recognize that SN-A is attempting the optional 3GPP AKA

10   (e.g., MODE = SHA-1), issue a user authentication reject, and await standard 3GPP AKA to establish a new SSK with SN-A.

      FIG. 15 is a flowchart of a process for using cryptographic data associated with different cells. As

15   shown, a MS stores (step 1502) cryptographic data, such as SSK/TSQN pairs, for different service networks. After determining (step 1504) a SN providing service, the MS can access and use the associated cryptographic data, for example, for authentication and encryption.

20   The techniques described above can, potentially, offer significant benefits for networks such as 3GPP and TR-45 (3GPP2) networks. For example, the techniques can allow for standard 3GPP AKA or modified 3GPP AKA at a service provider's discretion. The techniques can offer mutual

25   authentication based on a publicly scrutinized cryptographic primitive. Potentially, techniques can reduce HE/SN AV traffic when a common AKA primitive is shared between HE and SN. The techniques can reduce the probability of SQN re-synchronization problem by using

30   TSQN. The techniques can also reduce the need for SSD update in TR-45 networks, can reduce the vulnerability of fixed SSD by ensuring new SSK formation between MS and SN,

18

can reduce cryptographic export/import concerns for the
United States and other countries interested in adopting
TR-45 standards, and can reduce the need for VLR-to-VLR AV
sharing, SSD sharing, and SSD update for border cell

5   operations.

Other embodiments are within the scope of the
following claims. Additionally, though many of the method
claims feature a series of elements, the order these
elements occur may vary from their order in the claim.

WHAT IS CLAIMED IS:

        1.   A method for use in authenticating a service
network to a station, the station having a home environment
5 network, the method comprising:
        storing a key at the service network;
        transmitting information to the station from the
service network that enables the station to compute the key
stored at the service network;
10   receiving a request for service at the service network
from the station;
        adjusting a value corresponding to key usage; and
        transmitting information corresponding to the value to
the station.
15

        2.   The method of claim 1,
        further comprising receiving a vector of
authentication information from the home environment
network of the station, the vector including an indication
20 of the vector's position in a sequence of vectors; and
        wherein transmitting information to the station that
enables the station to compute the key stored at the
service network comprises transmitting portions of the
received vector of authentication information.
25

        3.   The method of claim 2, wherein the received vector
of authentication information comprises the key stored by
the service network.

30   4.   The method of claim 2, further comprising
computing at the service network the key stored by the

                            20

service network based on information included in the
received vector.

5.   The method of claim 1, wherein adjusting a value
indicating use of the key comprises incrementing a sequence
number corresponding to a number of times the key has been
used.

6.   The method of claim 5, wherein the value comprises
a TSQN (Temporary Sequence Number).

7.   The method of claim 1, wherein
      the station comprises a cellular phone; and
      the service network and home environment networks
comprise cellular networks.

8.   The method of claim 1, further comprising using
the key to compute a cipher key for encrypting
communication between the service network and the station.

9.   The method of claim 1, further comprising
negotiating use of a cryptographic primitive between the
service network and the home environment network.

10.   The method of claim 1, further comprising
      transmitting a challenge to the station;
      receiving a challenge response from the station; and
      comparing the received challenge response with an
expected response.

11.   The method of claim 1, further comprising:

computing the key stored by the service network at the
station;

receiving the information indicating the value
corresponding to key usage at the station; and

5   comparing the received value with a value
corresponding to key usage maintained by the station.

12.   A method for use in authenticating a service
network to a station, the station having a home environment
10   network, the method comprising:

receiving information at the station from the service
network;

computing a key based on the information received at
the station from the service network, the computed key also
15   being stored by the service network;

maintaining an indicator of key usage at the station;

receiving at the station an indicator of key usage
maintained by the service network; and

comparing the key usage indicator maintained by the
20   service network with the key usage indicator maintained by
the station.

13.   The method of claim 12, further comprising:

maintaining an authentication vector sequence number
25   at the station;

receiving at the station from the service network an
indication of an authentication vector sequence number
maintained by the home environment network; and

comparing the authentication vector sequence number
30   maintained by the home environment network with the
received authentication vector sequence number maintained
by the station.

14. The method of claim 13, further comprising receiving from the service network identification of a cryptographic primitive.

15. The method of claim 12, wherein
the station comprises a cellular phone; and
the service network and home environment network comprise cellular networks.

16. The method of claim 12, further comprising:
using the key to compute a cipher key for encrypting communication between the service network and the station.

17. The method of claim 12, further comprising:
receiving a challenge from the service network;
determining a challenge response; and
transmitting the challenge response to the service network.

18. The method of claim 12, wherein maintaining an indicator of key usage at the station comprises maintaining a key sequence number counter.

19. A method for use in authentication in a communications network including a home environment network, a service network, and a station, the method comprising:
determining at the home environment network a cryptographic primitive offered by the service network; and

based on the determined cryptographic primitive, transmitting to the service network at least one vector of authentication information corresponding to a particular station.

5

20. The method of claim 19, wherein determining comprises receiving identification of the cryptographic primitive from the service network.

10   21. The method of claim 20, wherein the identification comprises a value of a MODE field.

22. The method of claim 19, wherein the vector of authentication information comprises an indication of an

15 authentication vector sequence number maintained by the home environment network.

23. The method of claim 22, wherein the vector of authentication information comprises a challenge and an

20 expected response.

24. A method for use by a mobile station that can communicate with different service networks, the method comprising:

25   storing different sets of cryptographic information for the different respective service networks;

selecting a set of cryptographic information for one of the service networks; and

using the selected set of cryptographic information to

30 communicate with the service network.

25.   The method of claim 24, wherein the sets of cryptographic information comprise a key shared by the station and the service network.

26.   The method of claim 25, further comprising computing the key shared by the station and the service network based on information received from the service network.

27.   The method of claim 25, wherein the sets of cryptographic information comprise an indicator of usage of the key.

28.   The method of claim 27, wherein the indicator of usage comprises a sequence number.

29.   The method of claim 27, further comprising:

receiving from the service network an indicator of key usage; and

comparing the received indicator of key usage with the indicator of key usage included in the selected set of cryptographic information.

30.   The method of claim 25, wherein using the selected set of cryptographic information comprises using the selected set of cryptographic information to authenticate the service network.

31.   The method of claim 25, wherein using the selected set of cryptographic information comprises using the selected set of cryptographic information in encrypting communication between the station and the service network.

32. A method of handling authentication and key agreement in a system including a home environment network, a service network, and a mobile station, the home

5 environment network and the mobile station sharing a secret key K, the method comprising:

determining whether the home environment and the service network share a cryptographic primitive;

if it is determined that the home environment and the

10 service network do not share a cryptographic primitive, handling authentication and key agreement between the mobile station and the service network using 3GPP (Third Generation Project Partners) AKA (authentication and key agreement); and

15 if it is determined that the home environment and the service network share a cryptographic primitive, handling authentication and key agreement by:

computing a shared secret key (SSK);

transmitting information from the service network

20 to the station that enables the station to compute the SSK; and

replacing the use of K in the 3GPP AKA with SSK.

Abstract of the Disclosure

Techniques are described for enabling authentication and/or key agreement between communications network stations and service networks. The techniques described include the negotiation and use of a cryptographic primitive shared between a service network and a home environment of a station. The techniques described also feature a key usage indicator, such as a sequence number, maintained by the service network and a station. Comparison of the key usage indicators can, for example, permit efficient authentication of the service network.

FIG. 1/15
(Prior Art)

```
Generate SQN

Generate RAND
```

SQN MODE   RAND

K

f1   f2   f3   f4   f5
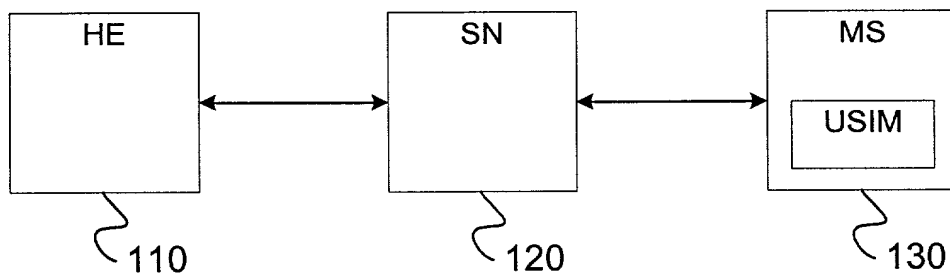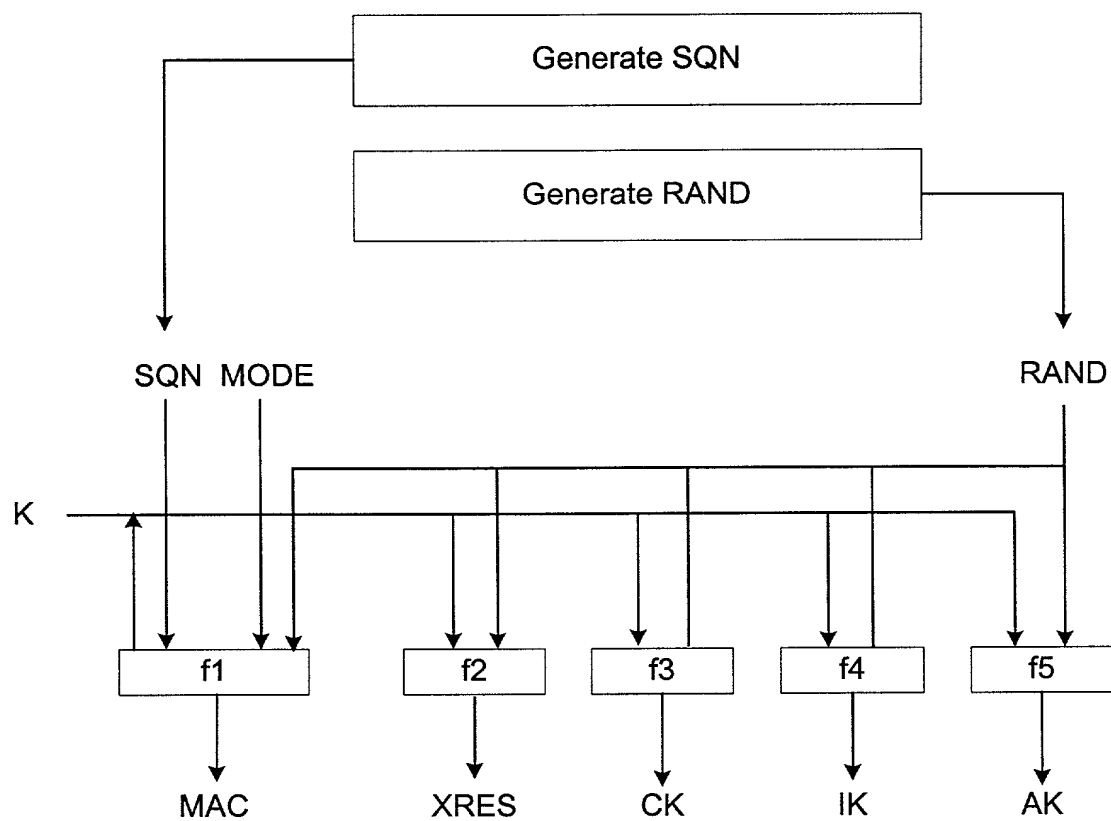
MAC   XRES   CK   IK   AK

AUTN := SQN XOR AK || MODE || MAC
AV := RAND || XRES || CK || IK || AUTN

FIG. 2/15
(Prior Art)

from SN

RAND SQN_{HE} XOR AK   MODE

f5

AK   XOR

SQN_{HE}

K

| f1 | f2 | f3 | f4 |
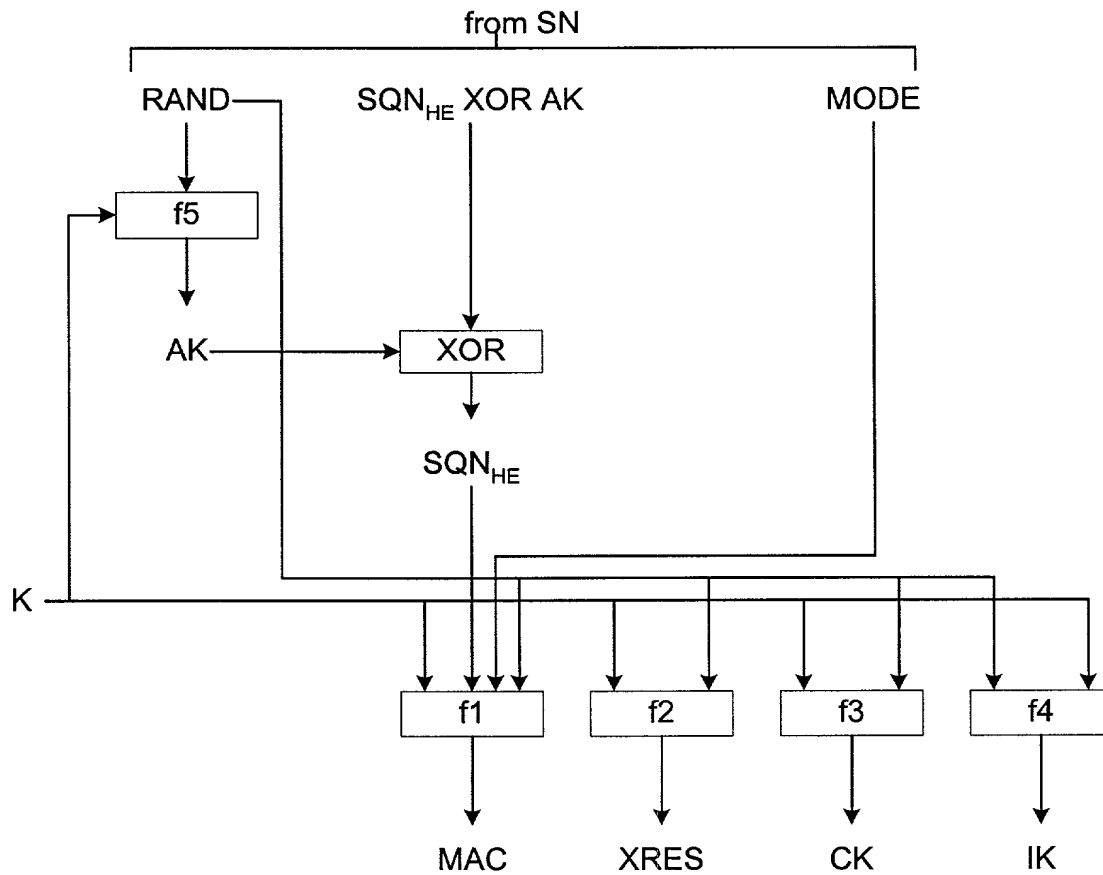
MAC   XRES   CK   IK

Verify MAC = XMAC
Verify $SQN_{HE} > SQN_{USIM/MS}$

FIG. 3/15
(Prior Art)

SN sends authentication data request to HE 〜 202

HE generates authentication vectors AV(1..n) 〜 204

HE sends AV(1..n) to SN 〜 206

SN stores authentication vectors 〜 208

SN selects authentication vector AV(i) 〜 210

SN sends RAND(i) and AUTN(i) to MS 〜 212

MS verifies AUTN(i) and computes RES(i) 〜 214

MS sends RES(i) to SN 〜 216

SN compares RES(i) and XRES(i) 〜 218

SN selects CK(i) and IK(i) MS computes CK(i) and IK(i) 〜 220

FIG. 4/15
(Prior Art)

FIG. 5/15
(Prior Art)

```
┌─────────────────────────┐
│ SN sends authentication data │        602
│ request to HE identifying   │ ∿/
│ AKA algorithm            │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ HE generates authentication │        604
│ vectors AV               │ ∿/
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ HE sends AV to SN        │ ∿/     606
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ SN stores authentication │        608
│ vector AV and generates  │ ∿/
│ SSK(i)                   │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ SN selects authentication │        610
│ vector                   │ ∿/
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ SN sends RAND(i) and     │        612
│ AUTN(i) to MS            │ ∿/
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ MS verifies AUTN(i) and  │        614
│ computes RES(i)          │ ∿/
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ MS sends RES(i) to SN    │ ∿/     616
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ SN compares RES(i) and   │        618
│ XRES(i)                  │ ∿/
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│ MS computes CK(i) and IK(i) │      620
│ SN selects CK(i) and IK(i)  │ ∿/
└─────────────────────────┘
```

FIG. 6/15

```
┌─────────────────────────┐
│   SN generates RAND(i)  │
│  SN uses SSK(i) to generate │ ～／ 702
│        TAUTN(i)         │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│    SN sends RAND(i) and │
│      TAUTN(i) to MS with │ ～／ 704
│        MODE=SHA-1       │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│   MS verifies TAUTN(i) and │ ～／ 706
│      computes RES(i)    │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│                         │
│    MS sends RES(i) to SN │ ～／ 708
│                         │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│   SN compares RES(i) and │ ～／ 710
│         XRES(i)         │
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│  MS computes CK(i) and IK(i) │ ～／ 712
└─────────────────────────┘
            │
            ▼
┌─────────────────────────┐
│  SN computes CK(i) and IK(i) │ ～／ 714
└─────────────────────────┘
```

FIG. 7/15

FIG. 8/15

from SN

RAND ——— TSQN$_{SN}$ XOR AK   MODE

f5

AK ———→ XOR

TSQN$_{SN}$

SSK

f1   f2   f3   f4

MAC   XRES   CK   IK

Verify MAC = XMAC
Verify TSQN$_{SN}$ > TSQN$_{USIM/MS}$

FIG. 9/15

IK   RAND

f3

SSK

FIG. 10/15

FIG. 11/15

```
                    ┌─────────────────────────────┐
                    │        Generate SQN         │
                    └─────────────────────────────┘

                    ┌─────────────────────────────┐
                    │        Generate RAND        │
                    └─────────────────────────────┘
```

SQN MODE   RAND

K

| f1 | f2 | f3 | f4 | f5 | f6 |

MAC   XRES   CK   IK   AK   SSK
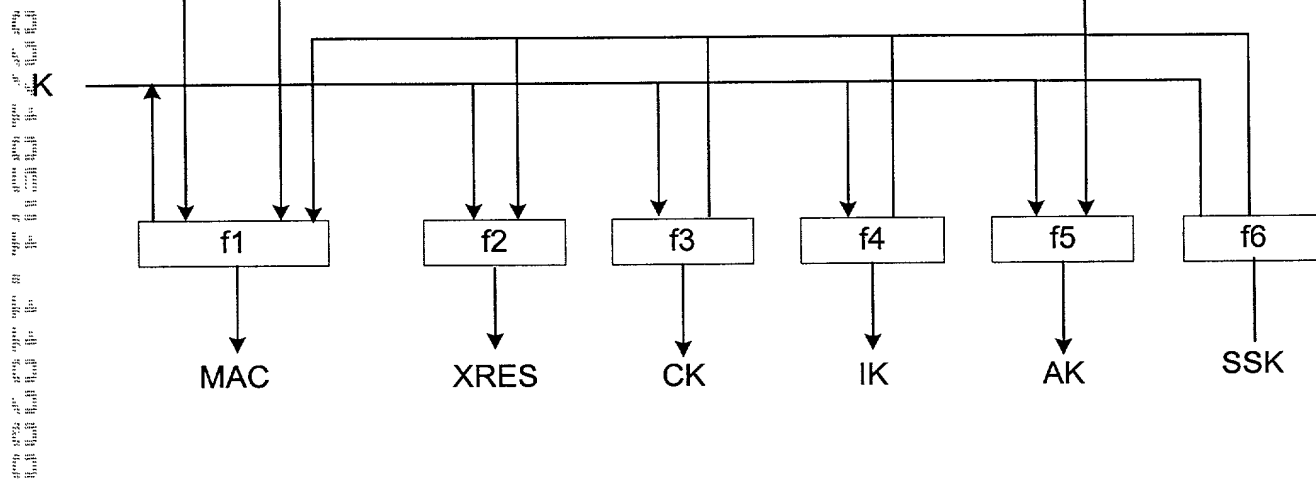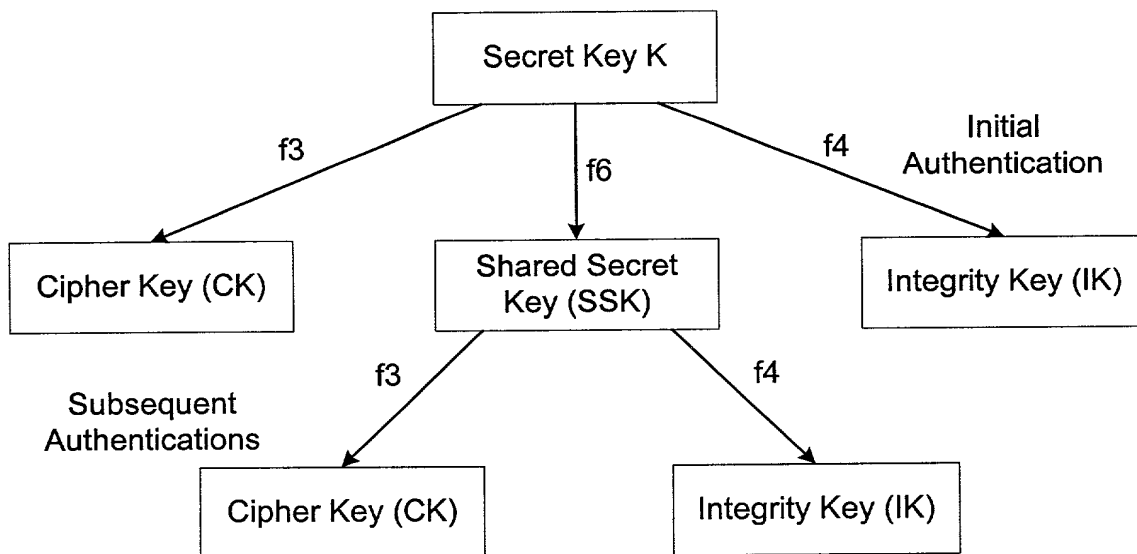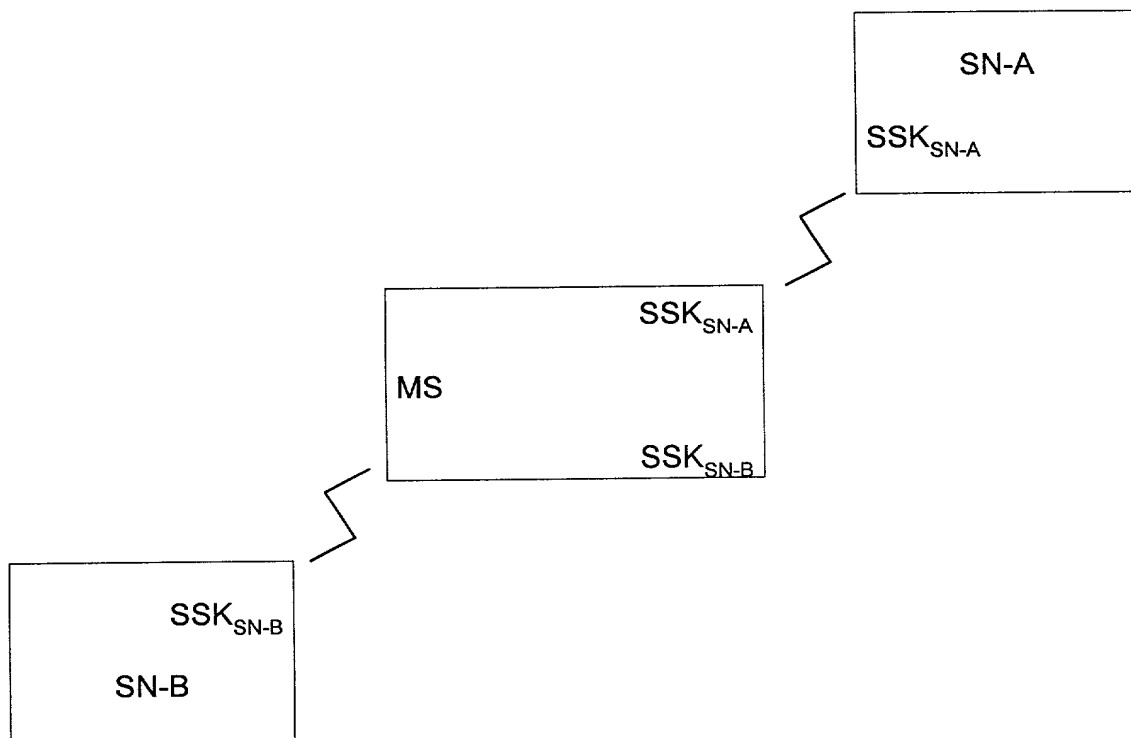
AUTN := SQN XOR AK || MODE || MAC
SSAV := RAND || XRES || CK || IK || SSK || AUTN

FIG. 12/15

FIG. 13/15

SN-A

SSK_{SN-A}

SSK_{SN-A}

MS

SSK_{SN-B}

SSK_{SN-B}

SN-B

FIG. 14/15

```
┌─────────────────────┐
│  store cryptographic │
│  data corresponding to│      ⌇ 1502
│  different service   │
│  networks            │
└─────────────────────┘
           │
           ▼
┌─────────────────────┐
│  determine service  │
│  network providing  │      ⌇ 1504
│  service            │
└─────────────────────┘
           │
           ▼
┌─────────────────────┐
│  use stored         │
│  cryptographic data │
│  corresponding to   │      ⌇ 1506
│  determined service │
│  network            │
└─────────────────────┘
```
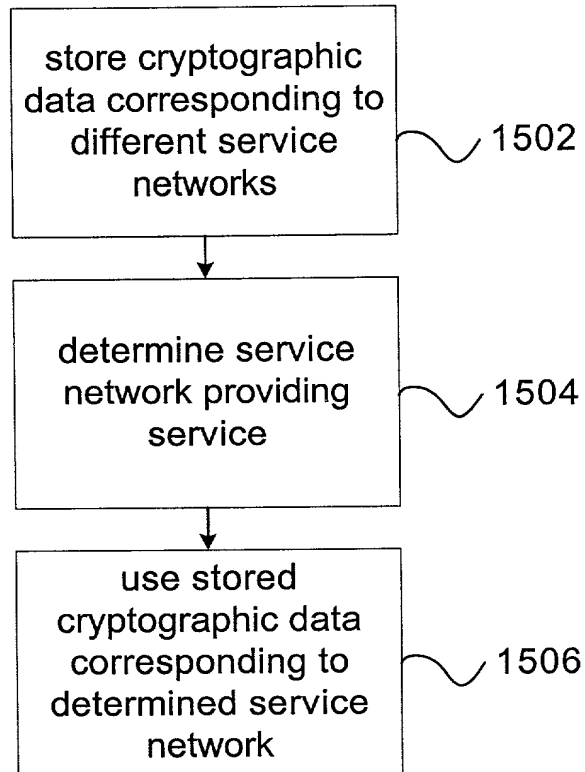
FIG. 15/15

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

<u>**Docket No. 99-956**</u>

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

CRYPTOGRAPHIC TECHNIQUES FOR A COMMUNICATIONS NETWORK

as Appln. Serial No.   And was amended on

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)   <u>Priority Claimed</u>

_____   _____   _____ [_] Yes [_] No

(Number)   (Country)   (Day/Month/Year filed)

I hereby claim the benefit under Title 35, United States Code, 119(e) of any United States provisional applications(s) listed below.

<u>60/165,539& 60/167,811</u>   <u>November 15 & 29, 1999</u>

(Application Number)   (Filing Date)

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date for this application:

_____   _____   _____

(Appln. Serial No.)   (Filing Date)   (Status—patented, pending, abandoned)

Docket No.**99-956**

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Leonard C. Suchyta, Reg. No. 25,707 and James K. Weixel Reg. No. 44,399

Address all telephone calls to   **James K. Weixel**   At telephone no.   **(781) 466-2220**

Address all correspondence to   **Leonard C. Suchyta**
                                     Verizon Services Group
                                     600 Hidden Ridge, HQE03G13
                                     Irving, TX 75038

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF INVENTOR   **Christopher Paul Carroll**

Inventor's signature   _Christopher Paul Carroll_   Date ___11/8/2000___

Residence   **Framingham, Massachusetts**   Citizenship   **USA**

Post Office Address   ~~146 Danforth Street Framingham, MA 01701~~   8 Village Green Lane, Natick MA 01760